WHAT IS CLAIMED IS:

1. A method for secure transmission of messages between at least two users of a telecommunications network, the method comprising:

generating a secret random binary encryption key using a key generator;

recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key, a first user of the at least two users receiving the first portable medium with the first recorded key and a second user of the at least two users receiving the second portable medium with the second recorded key;

inserting the first medium into a first reading device assigned to a first telecommunications device of the telecommunications network and inserting the second medium into a second reading device assigned to a second telecommunications device of the telecommunications network, and reading the first and second recorded keys using the first and second reading devices respectively;

establishing a connection between the first and second telecommunications devices;

checking the inserting and comparing the first and second recorded keys using a first logistics device and a second logistics device, the first logistics device being assigned to the first telecommunications device and the second logistics device being assigned to the second telecommunications device; and

upon a match in the comparing, encrypting the messages using at least a part of the key.

2. The method as recited in claim 1 wherein the reading the first and second recorded keys defines a first read key and a second read key respectively, and further comprising:

synchronizing the first and second read keys or parts of the first and second read keys using the first and second logistics devices respectively so as to encrypt and decrypt the messages.

3. The method as recited in claim 1 further comprising:

generating a plurality of additional secret random binary encryption keys using the key generator;

recording each of the plurality of additional secret keys on the first portable medium so as to define a plurality of additional recorded keys, each of the additional recorded keys being assigned to a respective connection between the first user and a respective other user of the at least two users;

inserting the first medium into the first reading device or another device assigned to the first telecommunications device;

selecting the assigned respective additional recorded key using the first reading device or the other device upon an establishing of the respective connection;

and encrypting the messages corresponding to the first user and the respective other user using the assigned respective additional recorded key.

4. The method as recited in claim 1 wherein an optical random number generator with a beam splitter is used for the generating.

5. The method as recited in claim 1 wherein a spontaneous emission of a photon in electrically or optically excited matter is used for the generating.

6. The method as recited in claim 1 wherein a physical noise-production process or a radioactive decay is used for the generating.

7. The method as recited in claim 1 wherein first key is recorded only on the first and second portable media.

8. The method as recited in claim 1 wherein the first and second portable media include at least one of a magnetic tape, a CD, and a suitable semiconductor storage device.

9. The method as recited in claim 1 further comprising additional portable media and wherein a number and/or a type of the additional portable media is freely selectable.

10. The method as recited in claim 1 wherein the key generator is accessible to a public.

11. The method as recited in claim 1 further comprising activating the key generator by inserting payment device or a magnetic strip card.

12. The method as recited in claim 1 wherein the key or parts of the key, is used only once.

13. An encryption system for secure transmission of messages between at least two users of a telecommunications network, the encryption system comprising:

a key generator for generating a random binary encryption key;

a recording device for recording the key on a first portable medium and a second portable medium so as to define a first and a second recorded key respectively;

a first reading device and a second reading device, the first and second reading devices for reading the first and second recorded keys respectively, the first reading device assigned to a first telecommunications device of the telecommunications network and the second reading device assigned to a second telecommunications device of the telecommunications network;

a first logistics device assigned to the first telecommunications device and a second logistics device assigned to the second telecommunications device, the first and second logistics devices for checking proper insertion of the first and second media in the first and second reading devices respectively, and for comparing the first and second recorded keys so as to seek a match; and

a first encryption and/or decryption device assigned to the first telecommunications device and a second encryption and/or decryption device

assigned to the second telecommunications device, the first and second encryption and/or decryption devices for encrypting and/or decrypting the messages using a least a part of the key if the first and second logistics devices determine a match.

14. The encryption system as recited in claim 13 wherein the reading the first and second recorded keys defines a first read key and a second read key respectively, and wherein the first and second logistics devices are capable of synchronizing the first and second read keys or parts of the first and second read keys.

15. The encryption system as recited in claim 13 wherein the key generator includes an optical random number generator having a beam splitter.

16. The encryption system as recited in claim 13 wherein the key generator includes a random number generator using a spontaneous emission of photons in electrically or optically excited matter.

17. The encryption system as recited in claim 13 wherein the key generator includes a random number generator using a physical noise-generating process or a radioactive decay.

18. The encryption system as recited in claim 13 further comprising additional portable media and wherein the key generator includes an input keyboard for entering a desired number and/or a type of additional portable media.

19. The encryption system as recited in claim 13 wherein at least one of the first and second reading devices is capable of reading a plurality of additional random binary encryption keys, each of the plurality of additional keys being assigned to a respective connection between the first user and another of the at least two users, the first logistics device being capable of assigning the respective one of the plurality of additional keys to the respective connection.